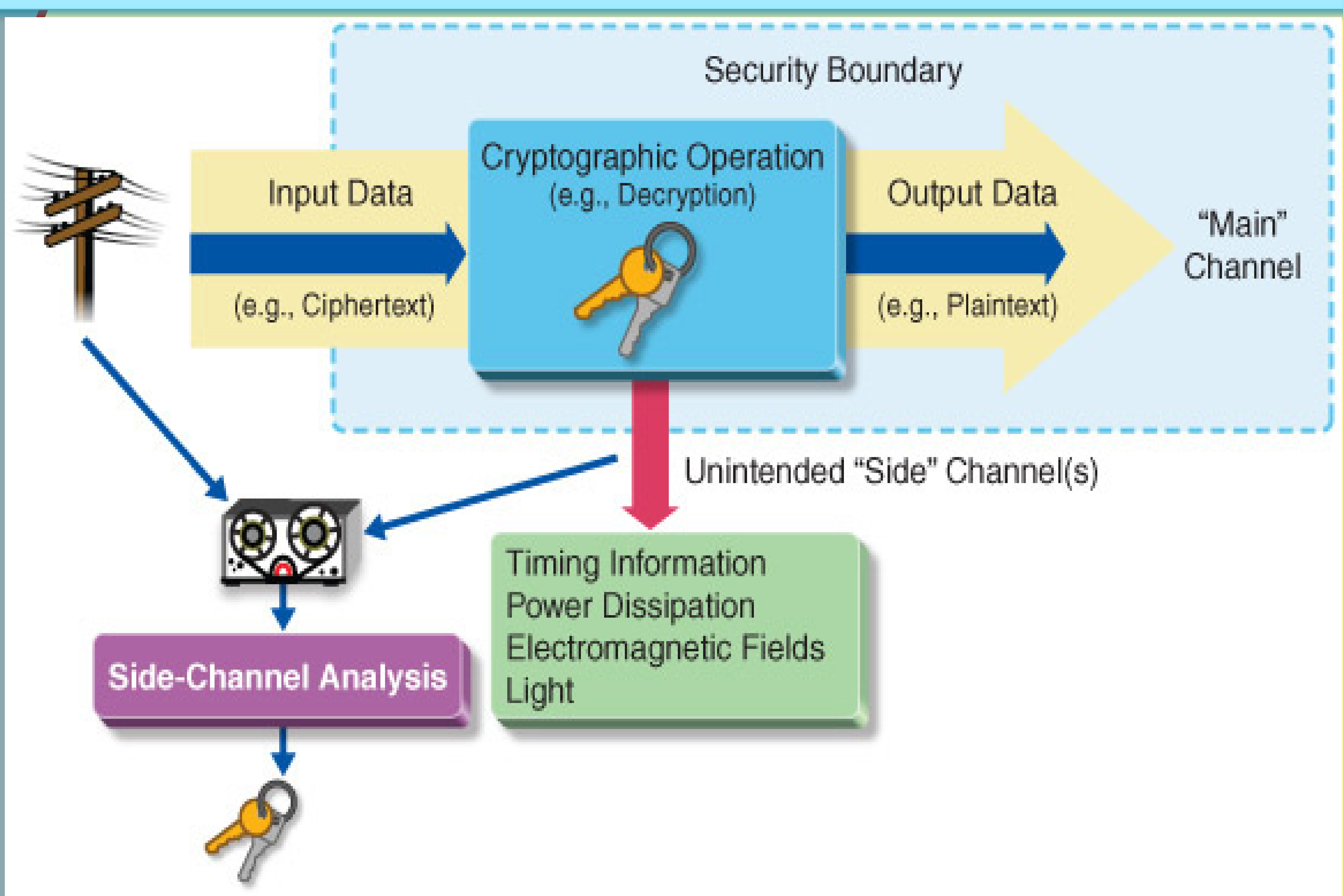
Medium: A Unified Statistics-based Framework for Analysis and Evaluation of Side-channel Attacks in Cryptosystems

PIs: Prof. Yunsi Fei and Aidong Ding, Northeastern University, Boston, MA

http://tescase.coe.neu.edu, y.fei@northeastern.edu

Side Channel Attack (SCA)



Use side-channel leakages to extract the secret key:

1. Power dissipation;
2. Cache timing information;
3. Electromagnetic leaks ;
4. Light emission.

Power SCA Model

The strongest statistical attack is the maximum-likelihood (ML-)attack whose success rate is given by a high-dimensional Gaussian distribution.

$$SR = \Phi_{\tilde{\Sigma}}\{\sqrt{n}\tilde{\mu}\}$$

For power leakage, ML-attack is equivalent to the CPA.

1st-order CPA: $L(t) = c + \varepsilon V + \sigma N(0,1), \quad SNR \quad \delta = \varepsilon / \sigma$

Success Rate Formula: $SR = \Phi_{\tilde{\Sigma}}\{\sqrt{n}\tilde{\mu}\} = \Phi_{\tilde{K}}\{\sqrt{n}\delta\vec{\kappa}/2\}$

Mean $\vec{\kappa}$: confusion vector of 2-way $\kappa(k_c, k_g)$ (On right)

Variance $\tilde{K}$: confusion matrix of three-way $\tilde{\kappa}(k_c, k_{g_i}, k_{g_j})$

J-th order CPA: $L(t_j) = c_j + \varepsilon_j V_j + \sigma_j N(0,1), \quad j = 1,\dots,J$

Success Rate Formula: $SR = \Phi_{\tilde{\Sigma}}\{\sqrt{n}\tilde{\mu}\} = \Phi_{\tilde{K}}\{\frac{\sqrt{n}\prod_{j=0}^{J}\delta_j}{2^{J-1}}\vec{\kappa}\}$

Cache-timing SCA Model

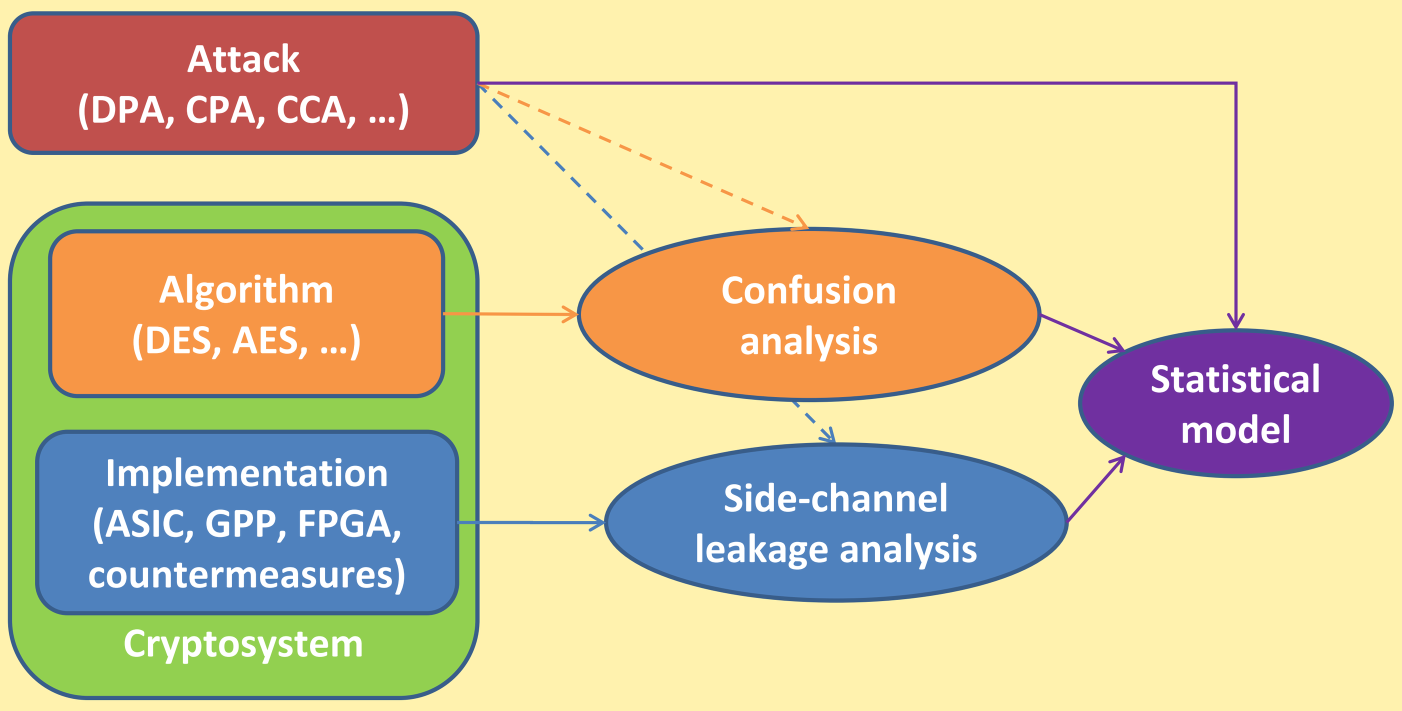
The attacker monitor n_L cache lines, with probability (p_0) of correctly identifying cache access in a total of n_A apparent accesses.

Success formula: $SR = \Phi_{\tilde{\Sigma}}\{\sqrt{n}\tilde{\mu}\}$

The mean elements: $\frac{1-p_0 n_L}{n_L - 1}(1-\frac{1}{n_L - 1})^{n_A - 1}$

The Variance elements also have explicit expression in those factors.

Modeling Framework



Algorithmic Confusion Analysis on DES/AES S-Box

Confusion coefficient: an algorithmic metric to reveal key distinguishability

Confusion coefficient between two keys (k_i, k_j):

$$\kappa = \kappa(k_i, k_j) = E[(V|k_i - V|k_j)^2]$$

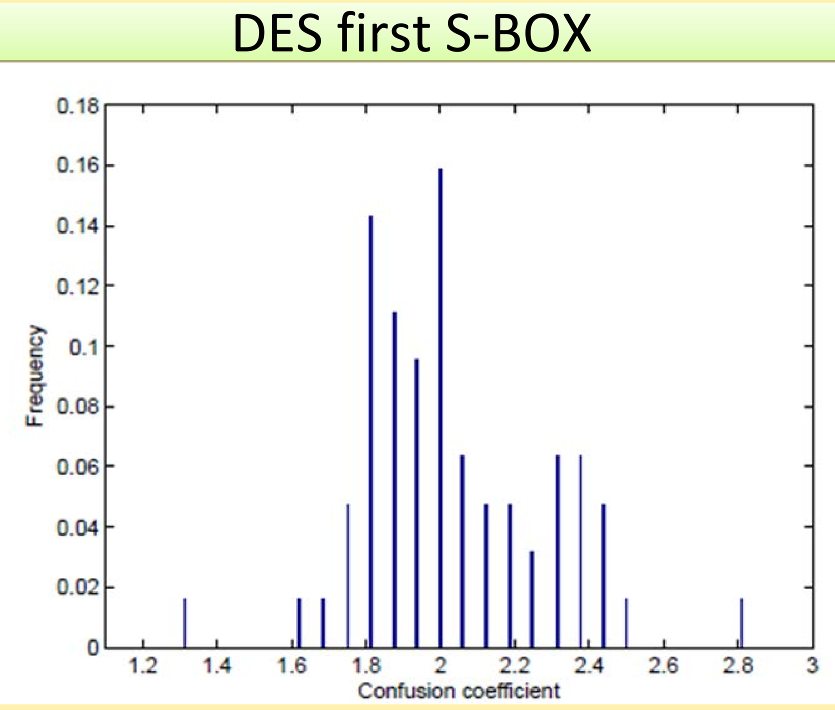
Three-way confusion coefficient:

$$\tilde{\kappa} = \tilde{\kappa}(k_h, k_i, k_j) = E[(V|k_h - V|k_i)(V|k_h - V|k_j)]$$

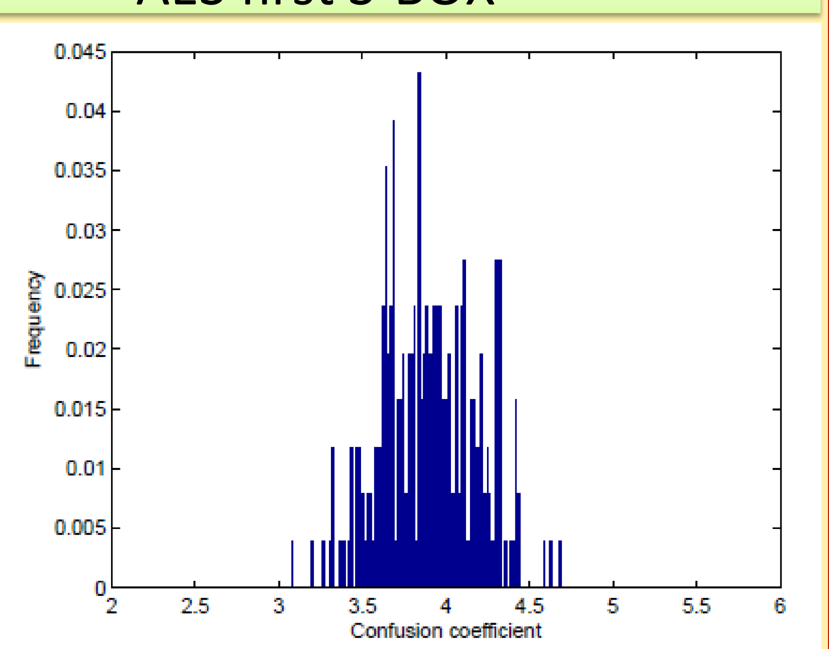
Confusion Lemma:

$$\tilde{\kappa}(k_h, k_i, k_j) = \frac{1}{2}[\kappa(k_h, k_i) + \kappa(k_h, k_j) - \kappa(k_i, k_j)]$$

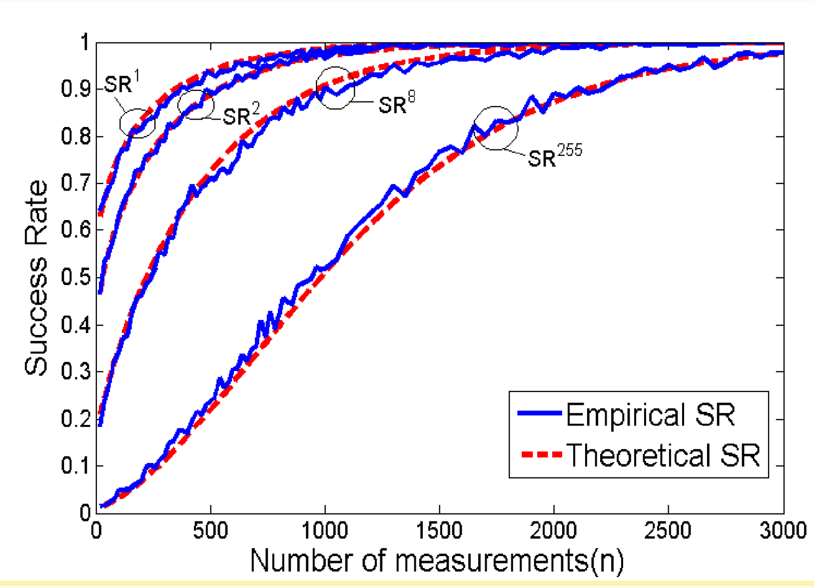
DES first S-BOX



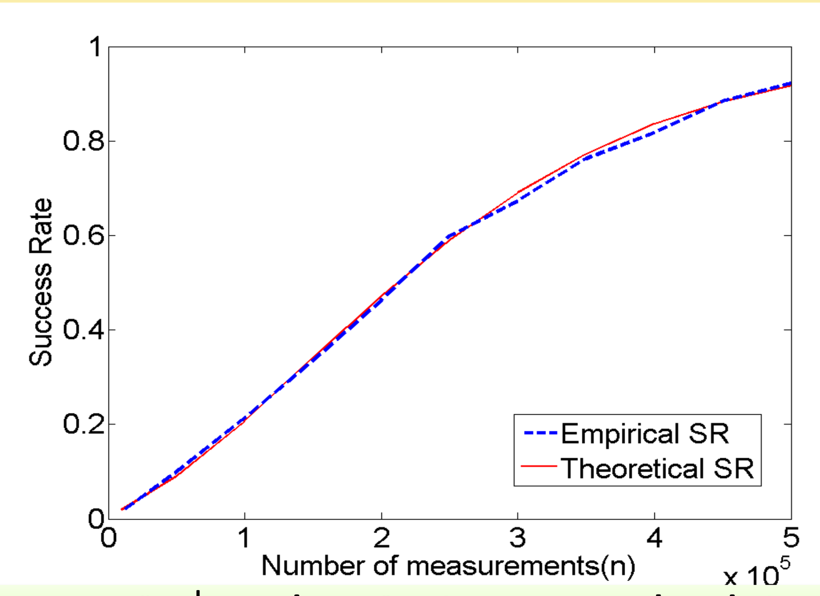
AES first S-BOX



Power SCA Experimental Results

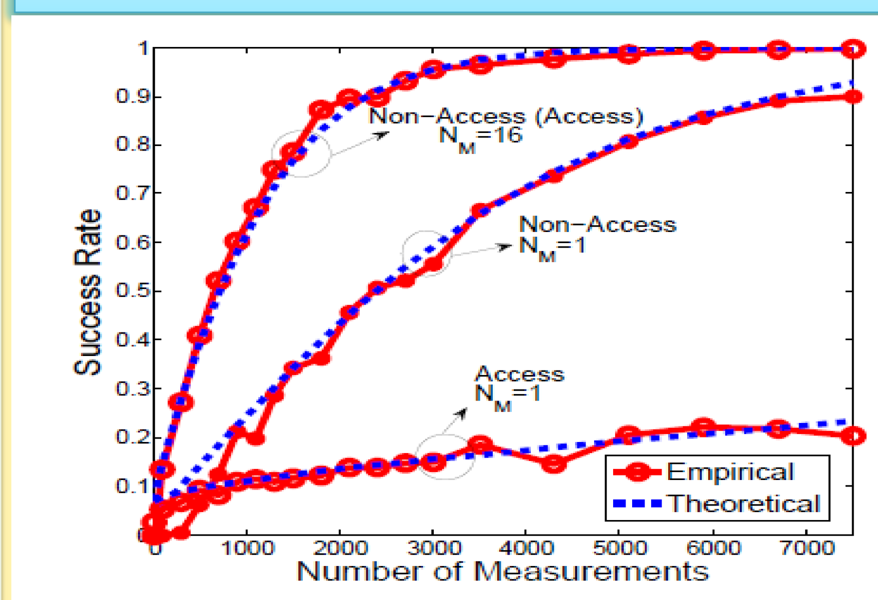


CPA on AES

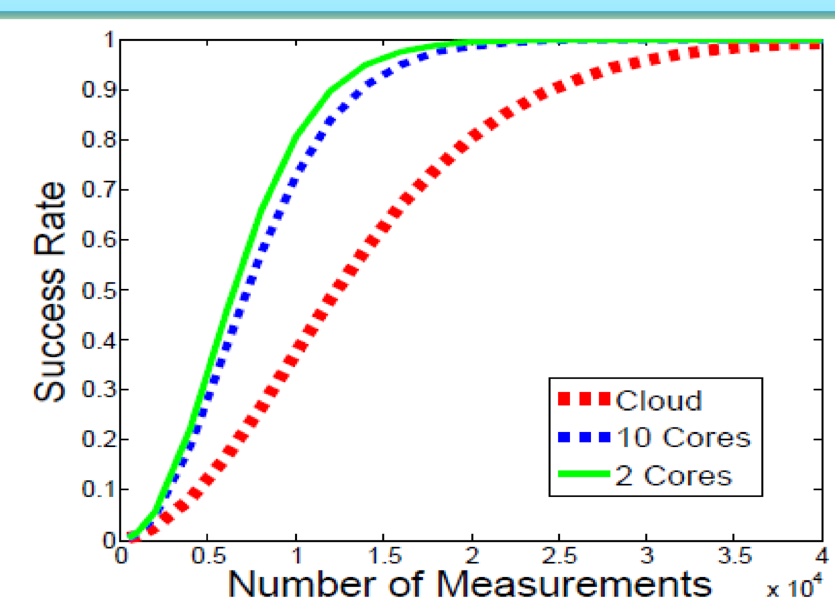


2nd-order CPA on masked AES

Cache SCA Experimental Results



Cache SCA on AES



Evaluation of different platforms

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia